

Notice of Allowability	Application No.	Applicant(s)
	09/638,616	TATEBAYASHI ET AL.
	Examiner Matthew T Henning	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to the communication filed October 12, 2004.
2. The allowed claim(s) is/are 1-10.
3. The drawings filed on 8/15/2000 are accepted by the Examiner.
4. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some* c) None of the:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) hereto or 2) to Paper No./Mail Date _____.
 - (b) including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. Notice of References Cited (PTO-892)
2. Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date 9/26/2003
4. Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. Notice of Informal Patent Application (PTO-152)
6. Interview Summary (PTO-413),
Paper No./Mail Date _____.
7. Examiner's Amendment/Comment
8. Examiner's Statement of Reasons for Allowance
9. Other _____.



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

1. This communication is in response to the communication filed 10/12/2004.

EXAMINER'S AMENDMENT

2. The application has been amended as follows:

The title of the invention is not descriptive of the invention claimed (See MPEP § 606.01), and therefore the title is amended to read as follows:

METHOD OF ENCRYPTION AND DECRYPTION WITH BLOCK NUMBER DEPENDANT KEY SETS, EACH SET HAVING A DIFFERENT NUMBER OF KEYS

Response to Arguments

3. Applicant traverses primarily that:

- i. Matsuzaki did not disclose taking in data one block at a time in order.
- ii. Matsuzaki did not disclose selecting a mode of operation according to the number of blocks previously processed.
- iii. Matsuzaki did not disclose generating two different groups of keys, in which one of the groups contains more keys than the other, and that each group was used for a different mode of operation.

4. Applicant's argument i. filed 10/12/2004, has been fully considered but is not persuasive. Matsuzaki did in fact disclose taking a block of 64 bits into the encryption device, as pointed out by the applicant on page 10 of the correspondence filed 10/12/2004.

5. Applicant's arguments, see ii, and iii, filed 10/12/2004, with respect to claims 14-6, and 9-10 have been fully considered and are persuasive. The rejection of claims 1-10 has been withdrawn.

Allowable Subject Matter

6. Claims 1-10 are allowed.

7. The following is an examiner's statement of reasons for allowance:

8. Matsuzaki et al. (US Patent Number 5,351,299), does not teach or suggest a combination as claimed in independent claims 1, 4-6, and 9-10, including a key generating step for generating a first group composed of a predetermined number n of different subkeys when a first mode is selected, and a second group composed of less than n different subkeys when the second mode is selected. As can be seen from Matsuzaki Fig. 6, there is only one mode of operation and one group of subkeys SK1. Therefore, claims 1, 4-6, and 9-10, are allowable over Matsuzaki.

9. Shimuzu et al. (US Patent Number 6,772,343) disclosed a encryption/decryption system in which even and odd numbered data blocks were submitted to two different modes of encryption with different keys. However, Shimuzu does not teach or suggest a combination as claimed in independent claims 1, 4-6, and 9-10, including a key generating step for generating a first group composed of a predetermined number n of different subkeys when a first mode is selected, and a second group composed of less than n different subkeys when the second mode is selected. As can be seen from Shimuzu Fig. 1, each group of keys contains an equal number of keys. Therefore, claims 1, 4-6, and 9-10, are allowable over Shimuzu.

10. Tajima et al. (US Patent Number 5,517,614) disclosed an encryption system in each block of data was encrypted according to an algorithm selected based on the previously

encrypted blocks of data. However, Tajima does not teach or suggest a combination as claimed in independent claims 1, 4-6, and 9-10, including the blocks being input into the encryption system in order one at a time. This can be seen from Tajima Fig. 1, in which the blocks are input simultaneously into a block processing section. Therefore, claims 1, 4-6, and 9-10, are allowable over Tajima.

11. Chou et al. (US Patent Number 5,081,676) disclosed a system for encryption in which two sets of keys were generated, and one set of the keys contained less keys than the other. However, Chou does not teach or suggest a combination as claimed in independent claims 1, 4-6, and 9-10, including the first set of keys being used for one mode of operation and the second set of keys being used for a second mode of operation. Instead, Chou disclosed that the two sets of keys were combined to create a single control key (See Chou Fig. 1 and Fig. 2). Therefore, claims 1, 4-6, and 9-10, are allowable over Chou.

12. Windirsch (US patent Number 6,760,439) disclosed a system in which multiple encryption algorithms may be performed simultaneously in a pipeline fashion. However, Windirsch does not teach or suggest a combination as claimed in independent claims 1, 4-6, and 9-10, including a key generating step for generating a first group composed of a predetermined number n of different subkeys when a first mode is selected, and a second group composed of less than n different subkeys when the second mode is selected. As disclosed by Windirsch, in Col. 6 Lines 55-63, the keys were not generated but instead they were pulled from storage, and also there was only one set of keys disclosed. Therefore, claims 1, 4-6, and 9-10, are allowable over Windirsch.

Art Unit: 2131

13. Claims 2-3, and 7-8 are allowable by virtue of their dependency to allowable claims 1, and 6.

14. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Matthew Henning
Assistant Patent Examiner
Art Unit 2131
3/2/2005



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER